GENERALIZATIONS IN THE THEORY OF NUMBERS AND THEORY OF LINEAR GROUPS.

By Mildred Sanderson.

1. **Condition for an inverse.** — The term function is here used to denote a rational integral function of y with integral coefficients. Employing a fixed integer m and a fixed function $P(y)$, we shall say that two functions are congruent modulis m and $P(y)$ if their difference can be given the form $mq(y) + P(y)Q(y)$; also that $f(y)$ has an inverse $f_1(y)$ if $f(y) \cdot f_1(y)$ is congruent to unity modulis m, $P(y)$. Then $f(y)$ and $f(y) + k(y)P(y)$ have the same inverse, so that we may restrict attention to functions of degree less than the degree r of $P(y)$. We proceed to prove the

Theorem. *If $P(y)$ is of degree r and is irreducible with respect to each prime factor of m, a function $R(y)$ of degree $< r$ has an inverse modulis m and $P(y)$ if and only if the greatest common divisor d of the coefficients of $R(y)$ is prime to m.*

We have $R(y) = dF(y)$. For any function $R_1(y)$, we may write

$$R(y)R_1(y) = dR_2(y) + P(y)Q(y),$$

where $R_2(y)$ is of degree $< r$. If R_1 is the inverse of R_1 then $dR_2(y) \equiv 1 \pmod{m}$, identically in y, so that d must be prime to m.

Conversely, if d is prime to m, $R(y)$ has an inverse modulis $m, P(y)$. We first prove by induction that $R(y)$ has an inverse modulis p^e, $P(y)$, where p is any prime factor of m, and e any positive integer. This is a well known fact for the case * $e = 1$. Assume that $R(y)$ has the inverse $R_1(y)$ modulis p^{e-1}, $P(y)$, so that

$$RR_1 = 1 + a(y)p^{e-1} + A(y)P(y).$$

Since R has an inverse modulis p, $P(y)$, we can choose $S(y)$ so that

$$RS(y) = -a(y) + pf(y) + F(y)P(y).$$

Then R is seen to have the inverse $R_1 + Sp^{e-1}$ modulis p^e, $P(y)$.

It remains to prove that if $R(y)$ has the inverse R_1 modulis m_1, $P(y)$, and the inverse R_2 modulis $m_2, P(y)$, where m_1 and m_2 are relatively prime,

*Serret, Algèbre, vol. 2, ch. 3, sec. 3; Dickson, Linear Groups, § 7.

then $R(y)$ has an inverse modulis $m = m_1 m_2, P(y)$. Set

$$RR_1 = 1 + m_1 a_1(y) + A_1(y)P(y), \quad RR_2 = 1 + m_2 a_2(y) + A_2(y)P(y).$$

Then

$$R(m_2 R_1 - m_1 R_2) = m_2 - m_1 + m(a_1 - a_2) + (m_2 A_1 - m_1 A_2)P(y).$$

Since $m_2 - m_1$ is prime to m, we can determine an integer k such that $k(m_2 - m_1) \equiv 1 \pmod{m}$. Then $k(m_2 R_1 - m_1 R_2)$ is an inverse of R modulis $m, P(y)$.

2. **Number of Classes of Residues Having an Inverse.**—Any function of y is congruent modulis $m, P(y)$ to a residue

$$a(y) = a_0 + a_1 y + \cdots + a_{r-1} y^{r-1}$$

each of whose coefficients a_i belongs to the set $0, 1, \cdots, m-1$. The number of ways of choosing r integers a_i from $0, 1, \cdots, m-1$, such that the greatest common divisor of the a_i is prime to m, is*

$$(1) \qquad n = [m, r] \equiv m^r \left(1 - \frac{1}{p_1^r}\right)\left(1 - \frac{1}{p_2^r}\right) \cdots \left(1 - \frac{1}{p_s^r}\right),$$

where $p_1, \cdots, p_s$ are the distinct prime factors of m. Hence there are exactly n classes of residues moduli $m, P(y)$, each having an inverse. The notation $\phi_r(m)$ is often used for this important generalization $[m, r]$ of Euler's function $\phi(m)$.

3. **Generalization of Fermat's Theorem.**—*If the remainder of degree $< r$ obtained on dividing $f(y)$ by $P(y)$ has coefficients whose greatest common divisor is prime to m, and if $P(y)$ is irreducible with respect to each prime factor of m, then*

$$(2) \qquad f^{[m,r]} \equiv 1 \ [\textit{modd } m, P(y)].$$

Denote by $R_1, \cdots, R_n$ the distinct residues having inverses modulis $m, P(y)$. Then $R_1 R_i, \cdots, R_n R_i$ are congruent to $R_1, \cdots, R_n$ in some order. Comparing the products, we get $R_i^n \equiv 1$ [modd $m, P(y)$].

For the case in which m is a prime p, we have $n = [p, r] = p^r - 1$. The theorem is thus a generalization also of Galois' theorem that

$$(3) \qquad f^{p^r - 1} \equiv 1 \ [\text{modd } p, P(y)],$$

if $f(y)$ is not divisible by $P(y)$ modulo p, and $P(y)$ is irreducible modulo p.

4. **Two-fold Generalization of Wilson's Theorem.**—*The product of the distinct residues $R_1, \cdots, R_n$, having inverses modulis $m, P(y)$, is congruent to*

*C. Jordan, Traité des substitutions, § 124.

-1 *when* m *is a power of an odd prime or twice the power of an odd prime, or when* $r = 1$, $m = 4$. *In all other cases, the product is congruent to* $+1$ *modulis* m, $P(y)$.

The product is congruent to $(-1)^{s/2}$, where s is the number of residues R_i whose square is congruent to unity. The proof is analogous to that of Gauss' generalization to any composite integral modulus of Wilson's theorem.

5. **Theorem.** *Let* $A(y)$ *and* $B(y)$ *be functions each of degree less than the degree of* $P(y)$, *which is irreducible with respect to each prime factor of* m. *If* m *and the coefficients of* $A(y)$, $B(y)$ *do not all have a common factor, there exist functions* $\alpha(y)$, $\beta(y)$ *such that*

$$\alpha(y)A(y) + \beta(y)B(y) \equiv 1 \quad [\text{mod}d\, m, P(y)]. \tag{4}$$

Let $A(y) = aA_1(y)$, $B(y) = bB_1(y)$, where the greatest common divisor of the coefficients of $A_1(y)$ is prime to m, likewise that for $B_1(y)$. Since the greatest common divisor of a, b, m is 1, there exist integers a_1, b_1 for which $a_1a + b_1b \equiv 1 \pmod m$. Then $\alpha(y) = a_1A_1^{-1}(y)$, $\beta(y) = b_1B_1^{-1}(y)$ satisfy (4).

6. **Theorem.** *There exists a function* $P(y)$ *of any assigned degree* r *which is irreducible with respect to any assigned prime moduli* $p_1, \cdots, p_s$.

As well known, there exists a function $P_i(y)$ of degree r irreducible modulo p_i. We may take

$$P(y) = \sum_{i=1}^{s} p_1 \cdots p_{i-1}p_{i+1} \cdots p_s P_i(y). \tag{5}$$

7. **Generalized Linear Substitutions.**—We consider substitutions

$$x_i' \equiv \sum_{j=1}^{v} c_{ij}(y)x_j \,[\text{modd}\, m, P(y)] \qquad (i = 1, \cdots, v), \tag{6}$$

in which the $c_{ij}(y)$ are rational integral functions of y with integral coefficients such that the determinant $|c_{ij}(y)|$ has an inverse modulis $m, P(y)$. Then the substitution has an inverse. Every such substitution is the product of substitutions of two elementary types, the one altering only one variable x_i, replacing it by $x_i + c(y)x_j$; the other altering only one variable, multiplying it by a function $l(y)$ having an inverse.

The order of the group $G(m, r, v)$ of all the substitutions (6) is

$$\Omega(m, r, v) = [m, rv]m^{r(v-1)}[m, r(v-1)]m^{r(v-2)} \cdots [m, r].$$

If $m = m_1m_2$, where m_1 and m_2 are relatively prime, the group G is the direct product of the permutable groups H_1, H_2, where H_k is the group composed of the substitutions

$$x_i' \equiv x_i + m_k \Sigma\, d_{ij}(y)x_j \,[\text{modd}\, m, P(y)].$$

The group H_1 is simply isomorphic with the group $G(m_2, r, v)$.

It remains to treat the case in which $m = p^e$, where p is a prime. The factors of composition of $G(p^e, r, v)$ are those of $G(p, r, v)$ and a certain number of p's.

The proofs of the preceding results are similar to that for the case of a single modulus m, C. Jordan, Traité des substitutions, pp. 93–105. The final group $G(p, r, v)$ has been discussed by L. E. Dickson, Linear Groups, p. 81, and Annals of Mathematics, 1, vol. 11 (1897), p. 169.

THE UNIVERSITY OF CHICAGO, May, 1911.